

.....
(Original Signature of Member)

117TH CONGRESS
1ST SESSION

H. R. 1833

To amend the Homeland Security Act of 2002 to provide for the responsibility of the Cybersecurity and Infrastructure Security Agency to maintain capabilities to identify threats to industrial control systems, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. Katko introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To amend the Homeland Security Act of 2002 to provide for the responsibility of the Cybersecurity and Infrastructure Security Agency to maintain capabilities to identify threats to industrial control systems, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “DHS Industrial Con-
5 trol Systems Capabilities Enhancement Act of 2021”.

1 **SEC. 2. CAPABILITIES OF THE CYBERSECURITY AND INFRA-**
2 **STRUCTURE SECURITY AGENCY TO IDENTIFY**
3 **THREATS TO INDUSTRIAL CONTROL SYS-**
4 **TEMS.**

5 (a) IN GENERAL.—Section 2209 of the Homeland
6 Security Act of 2002 (6 U.S.C. 659) is amended—

7 (1) in subsection (e)(1)—

8 (A) in subparagraph (G), by striking
9 “and” after the semicolon;

10 (B) in subparagraph (H), by inserting
11 “and” after the semicolon; and

12 (C) by adding at the end the following new
13 subparagraph:

14 “(I) activities of the Center address the se-
15 curity of both information technology and oper-
16 ational technology, including industrial control
17 systems;”; and

18 (2) by adding at the end the following new sub-
19 section:

20 “(p) INDUSTRIAL CONTROL SYSTEMS.—The Director
21 shall maintain capabilities to identify and address threats
22 and vulnerabilities to products and technologies intended
23 for use in the automated control of critical infrastructure
24 processes. In carrying out this subsection, the Director
25 shall—

1 “(1) lead Federal Government efforts to iden-
2 tify and mitigate cybersecurity threats to industrial
3 control systems, including supervisory control and
4 data acquisition systems;

5 “(2) maintain threat hunting and incident re-
6 sponse capabilities to respond to industrial control
7 system cybersecurity risks and incidents;

8 “(3) provide cybersecurity technical assistance
9 to industry end-users, product manufacturers, other
10 Federal agencies, and other industrial control system
11 stakeholders to identify, evaluate, assess, and miti-
12 gate vulnerabilities;

13 “(4) collect, coordinate, and provide vulner-
14 ability information to the industrial control systems
15 community by, as appropriate, working closely with
16 security researchers, industry end-users, product
17 manufacturers, other Federal agencies, and other in-
18 dustrial control systems stakeholders; and

19 “(5) conduct such other efforts and assistance
20 as the Secretary determines appropriate.”.

21 (b) REPORT TO CONGRESS.—Not later than 180 days
22 after the date of the enactment of this Act and every six
23 months thereafter during the subsequent 4-year period,
24 the Director of the Cybersecurity and Infrastructure Secu-
25 rity Agency of the Department of Homeland Security shall

1 provide to the Committee on Homeland Security of the
2 House of Representatives and the Committee on Home-
3 land Security and Governmental Affairs of the Senate a
4 briefing on the industrial control systems capabilities of
5 the Agency under section 2209 of the Homeland Security
6 Act of 2002 (6 U.S.C. 659), as amended by subsection
7 (a).